Espacenet

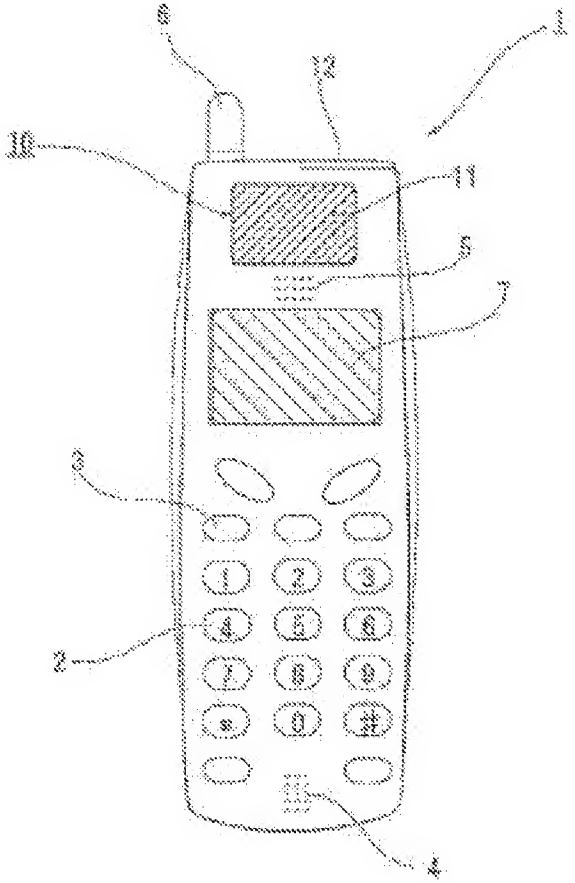
Bibliographic data: JP 2002082914 (A)

PERSONAL IDENTIFICATION DEVICE AND PERSONAL IDENTIFICATION METHOD

Publication date:	2002-03-22	
Inventor(s):	MATSUZAKI RUMIKO; NAKAYAMA SHUNICHI; TSUKADA ETSUJI; TAKIMOTO KEIICHIRO; TAKAHASHI TOMOKI ±	
Applicant(s):	NIPPON TELEGRAPH & TELEPHONE; MITSUBISHI RES INST INC ±	
Classification:	- international:	***G06F15/00; G06F21/20; H04L9/32; H04M1/00; H04M1/274; H04M1/2745; H04M1/275; H04M1/725; H04M11/00; H04Q7/38;*** (IPC1-7): G06F15/00; H04L9/32; H04M1/00; H04M1/274; H04M1/725; H04M11/00; H04Q7/38
	- European:	
Application number:	JP20000273604 20000908	
Priority number (s):	JP20000273604 20000908	

Abstract of JP 2002082914 (A)

PROBLEM TO BE SOLVED: To provide a personal identification device and a personal identification method by which access rights to various equipments and services can be established uniformly and inexpensively. SOLUTION: This personal identification device is composed of a portable terminal 1 on which fingerprint identification devices 10 and 13 and a radio transmitter 12 are mounted. The fingerprint authentication device is provided with a fingerprint detecting means 11 for detecting fingerprints, a fingerprint storing means for storing the fingerprint information of the user, and a fingerprint collating means for collating the fingerprint detected by the fingerprint detecting means with the fingerprint information stored in the fingerprint storing means. When the fingerprint collating means judges that the fingerprint detection information is made coincident with the fingerprint registration information, the radio transmitter transmits an access permission signal to external equipment. Thus, the legal user of the portable equipment/terminal can ensure an access right to a product on the market or provided service by performing personal identification by collating the fingerprint of the user himself or herself with the fingerprint registration information by the fingerprint authentication device of the portable equipment/terminal, and transmitting the access permission signal from the radio transmitter to the receiver.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－82914
（P2002－82914A）
(43)公開日　平成14年３月22日(2002.3.22)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｆ	５Ｂ０８５
Ｈ０４Ｑ	7/38		Ｈ０４Ｍ	1/00	Ｒ	５Ｊ１０４
Ｈ０４Ｌ	9/32			1/274		５Ｋ０２７
Ｈ０４Ｍ	1/00			1/725		５Ｋ０３６
	1/274			11/00	３０２	５Ｋ０６７

審査請求　未請求　請求項の数12　ＯＬ　（全　９　頁）　最終頁に続く

(21)出願番号　特願2000－273604(P2000－273604)

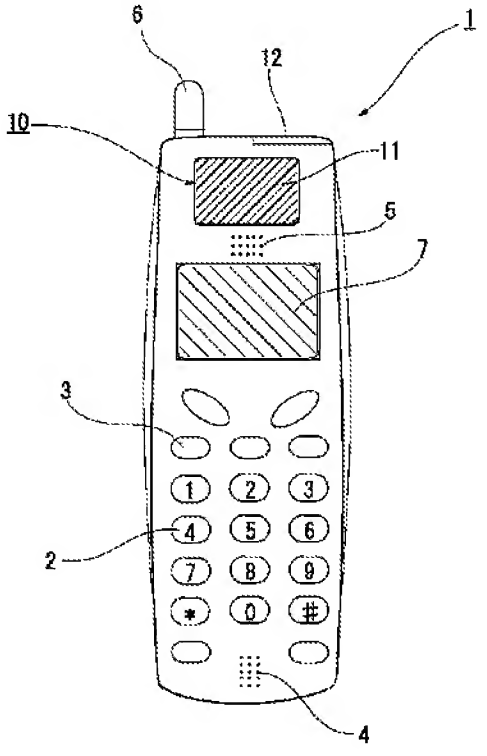
(22)出願日　平成12年９月８日(2000.9.8)

(71)出願人　399040405
東日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(71)出願人　591115475
株式会社三菱総合研究所
東京都千代田区大手町２丁目３番６号
(72)発明者　松崎　留美子
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(74)代理人　100094335
弁理士　島添　芳彦

最終頁に続く

(54)【発明の名称】　本人認証装置及び本人認証方法

(57)【要約】
【課題】　各種機器及びサービスへのアクセス権を一元的且つ集約的に確立し得る本人認証装置及び本人認証方法を提供する。
【解決手段】　本人認証装置は、指紋認証装置１０、１３及び無線発信装置１２を搭載した携帯機器／端末１からなる。指紋認証装置は、指紋を検出する指紋検出手段１１と、ユーザの指紋情報を記憶する指紋記憶手段と、指紋検出手段によって検出された指紋と指紋記憶手段に記憶された指紋情報とを照合する指紋照合手段とを備える。指紋照合手段が指紋検出情報及び指紋登録情報の一致を判定したとき、無線発信装置は、アクセス許可信号を外部機器に発信する。携帯機器／端末の正規ユーザ等は、携帯機器／端末の指紋認証装置によって本人の指紋を指紋登録情報情報と照合して本人認証を行った上で、その無線発信装置からアクセス許可信号を受信装置に送信し、これにより、販売製品又は提供役務に対するアクセス権を確保する。



【特許請求の範囲】
【請求項１】　指紋認証装置及び無線発信装置を搭載した携帯機器／端末により構成され、
前記指紋認証装置は、指紋を検出する指紋検出手段と、本人の指紋情報を記憶する指紋記憶手段と、前記指紋検出手段によって検出された指紋と前記指紋記憶手段に記憶された指紋情報とを照合する指紋照合手段とを備え、前記無線発信装置は、前記指紋照合手段が前記指紋及び指紋情報の一致を判定したときにアクセス許可信号を外部機器に発信することを特徴とする本人認証装置。
【請求項２】　前記指紋検出手段は、携帯機器／端末の外装部材に一体的に取付けられた静電容量式又は光学式の指紋認証センサにより構成されることを特徴とする請求項１に記載の本人認証装置。
【請求項３】　前記指紋照合手段は、前記指紋認証センサに組み込まれることを特徴とする請求項２に記載の本人認証装置。
【請求項４】　前記携帯機器／端末は、前記指紋記憶手段を備えたＩＣカードを有することを特徴とする請求項２に記載の本人認証装置。
【請求項５】　前記指紋照合手段は、前記ＩＣカードに組み込まれることを特徴とする請求項４に記載の本人認証装置。
【請求項６】　前記アクセス許可信号を送信すべき外部機器の情報を記憶した外部機器情報記憶手段を更に備えることを特徴とする請求項１乃至５のいずれか１項に記載の本人認証装置。
【請求項７】　前記無線発信装置は、アクセス権を要する役務又は機器の提供者側に属する受信装置と通信可能な近距離無線発信装置からなることを特徴とする請求項１乃至６のいずれか１項に記載の本人認証装置。
【請求項８】　指紋認証装置及び無線発信装置を搭載した携帯機器／端末と、前記無線発信装置と通信可能な受信装置とを使用し、前記携帯機器／端末の所持者の指紋を該携帯機器／端末の指紋情報記憶と照合して本人認証を行い、該本人認証の結果として本人確認がなされた場合に前記無線発信装置からアクセス許可信号を前記受信装置に送信し、該受信装置が関連する販売製品又は提供役務に対する本人のアクセスを可能にすることを特徴とする本人認証方法。
【請求項９】　前記受信装置は、前記無線発信装置が発信するアクセス許可信号を識別し、販売製品又は提供役務のセキュリティシステムを適宜解除し、これを利用可能な状態に移行することを特徴とする請求項８に記載の本人認証方法。
【請求項１０】　前記携帯機器／端末は、携帯電話機又はＰＨＳ電話機からなり、前記電話機の電話会社は、該電話機の指紋認証機能を利用した製品購入又は役務提供に対する対価を課金情報として集計し、前記製品の販売者又は役務提供者に代行して、集計後の対価合計を前記電話機の所有者又は契約者に請求することを特徴とする請求項８又は９に記載の本人認証方法。
【請求項１１】　前記電話会社は、前記電話機の利用料金と一緒に前記対価を前記所有者又は契約者に請求することを特徴とする請求項１０に記載の本人認証方法。
【請求項１２】　ＡＴＭ等の金融機関端末から所望の金額を電子マネーとして前記携帯機器／端末にチャージし、チャージした金額の範囲内において製品購入又は役務提供を可能にすることを特徴とする請求項８又は９に記載の本人認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、本人認証装置及び本人認証方法に関するものであり、より詳細には、携帯電話機等の携帯機器／端末に適用可能な指紋認証技術によって携帯機器／端末の所有者又は正規ユーザの本人認証を行い、各種機器及びサービスへのアクセス権を一元的且つ集約的に確立し得る本人認証装置及び本人認証方法に関するものである。
【０００２】
【従来の技術】従来、建築物又は車両等の出入口又はドア等の施錠機器として、金属製の鍵、カードキー、或いは、数字入力式施錠機器などが広く実用に供されてきた。近年において、ＩＣカード方式、音声認識方式又は虹彩認識方式等の多様な形式の施錠機器が開発されているが、この種の特殊構造の施錠機器は、極めて高価であり、現状では、一部の特殊なドア等に限定的に使用し得るにすぎない。
【０００３】クレジットカード又はキャッシュカード等が近年広く普及しているが、これらの各種カード類では、本人確認は、サイン又は暗証番号の照合に依存しており、このため、カードの偽造等による不正使用が、今日では、社会問題として深刻化している。
【０００４】また、インターネット等の公衆メディアを媒体とした電子商取引市場が近年急速に普及しつつある。この種のネットワークを使用した商取引においては、本人確認は、ネットワークを介して情報伝達可能なＩＤ番号及びパスワードや、電子証明書等の電子情報に基づいて実施される。このため、ＩＤ番号及びパスワード等を十分に管理し得ない場合、最も基本となる本人確認の信頼性及び確実性を担保し難く、電子商取引の安全性確保は、極めて困難である。
【０００５】かくして、キー又はカード等を使用した施錠又は金銭授受等においては、キー又はカードの偽造等の問題を完全には回避し難く、また、インターネット等を媒体とした電子商取引や、今後実用化されるであろう公的書類の電子申請及び電子交付システム等にあっては、ＩＤ番号及びパスワード等のデジタル情報の照合により本人確認を行うほかはなく、このため、本人確認を確実に実施可能な認証手段の開発が要望されている。

【０００６】
【発明が解決しようとする課題】信頼性及び確実性が高い本人認証手段として、個人の生物学的な特徴である指紋を認証する指紋認証技術の応用は、偽造又は盗用不能な認証方式として非常に有利である。指紋認証技術は、バイオメトリクス技術の一種であるが、本人認証の信頼度が極めて高いことから、多くのセキュリティシステムに対する今後の利用が期待されており、薄く且つ小型の指紋認証センサが現在、研究・開発されている。
【０００７】しかしながら、比較的利用頻度が高い個々の機器全てに指紋認証センサを搭載し又は装備することは、金銭的観点からも、個々の機器への本人の指紋登録に費やす時間及び手間等の現実的な観点からも、事実上、極めて困難である。このため、この種の本人認証方式を実用化するには、各種機器及びサービスへのアクセス権を一元的且つ集約的に確立し得る利便性を確保する必要があり、これを実現可能な新規システムの開発が要望される。
【０００８】本発明は、かかる事情に鑑みてなされたものであり、その目的とするところは、各種機器及びサービスへのアクセス権を一元的且つ集約的に確立し得る本人認証装置及び本人認証方法を提供することにある。
【０００９】
【課題を解決するための手段及び作用】本発明者は、上記目的を達成すべく、鋭意研究を重ねた結果、多数の消費者が常時携帯し且つ所有者個人に対する属性又は直接的な関連性が非常に高い機器として、携帯電話機（携帯電話器）、ＰＨＳ（Personal Handyphone System）電話機、ＰＤＡ(Personal Digital Assistant)等の携帯機器／端末に着目し、指紋認証センサを各携帯機器／端末に装着するとともに、携帯機器／端末の駆動源及び制御回路等を有効利用して各種機器又はサービスへのアクセス権を一元的且つ集約的に確立し得ることを見い出し、本発明を達成したものである。
【００１０】即ち、本発明によれば、本人認証装置は、指紋認証装置及び無線発信装置を搭載した携帯機器／端末により構成される。指紋認証装置は、指紋を検出する指紋検出手段と、本人の指紋情報を記憶する指紋記憶手段と、指紋を照合する指紋照合手段とを備える。指紋照合手段は、指紋検出手段によって検出された指紋情報と、指紋記憶手段に予め記憶された指紋情報とを照合する。無線発信装置は、指紋照合手段が指紋情報の一致を判定したときにアクセス許可信号を外部機器に発信する。
【００１１】本発明の上記構成によれば、指紋認証装置は、携帯機器／端末の所持者の指紋を所有者等の本人の指紋情報と照合して一致・不一致を判定し、無線発信装置は、指紋認証装置が指紋一致を判定したとき、外部機器にアクセス許可信号を発信する。アクセス許可信号を受信した外部機器は、指紋認証による本人認証に基づき、機器へのアクセス又はサービス利用を可能にする。従って、上記構成の本人認証装置によれば、携帯機器／端末の所有者等（本人）は、常時携帯可能な利便性を有する単一の機器、即ち、携帯電話機等の携帯機器／端末を常時携帯することにより、機械的施錠の解錠、電子機器又は通信機器のアクセスコードの解除、各種製品の購入、或いは、有料サービスの利用権等、即ち、各種機器又はサービスに対するアクセス権を一元的且つ任意の時期に得ることができる。
【００１２】本発明は又、指紋認証装置及び無線発信装置を搭載した携帯機器／端末と、無線発信装置と通信可能な受信装置とを使用した本人認証方法を提供する。殊に、本発明の本人認証方法は、携帯機器／端末の所持者の指紋を該携帯機器／端末の指紋情報記憶と照合して本人認証を行い、該本人認証の結果として本人確認がなされた場合に無線発信装置からアクセス許可信号を受信装置に送信し、受信装置が関連する販売製品又は提供役務に対する本人のアクセスを可能にすることを特徴とする。
【００１３】このような本発明の構成によれば、機器又はサービスの利用者本人と対応する携帯機器／端末の属性を有効利用して本人認証を行い、アクセス権を要するハードウェア（車両ドア、自宅ドア、ユーザ限定機器等）、或いは、アクセス権を要するサービス（Ｅコマース又は電子商取引等）の側に属する受信装置の属性を利用して機器又はサービスへのアクセスを適宜可能にする。携帯機器／端末は、所有者等の特定の指紋情報を記憶して指紋認証を行うので、受信装置は、携帯電話機の側において既に実施された本人認証の結果を受信すれば良い。即ち、機器又はサービスを提供する側の装置は、各個人の指紋情報を記憶又は登録する必要がなく、受信したアクセス許可信号の種別等のみを判定すれば良い。したがって、指紋認証によりセキュリティ機能を向上し得るばかりでなく、同様なセキュリティレベルを達成する従来のシステムに比べて、装置又は設備の初期投資又は維持管理費を大幅に軽減することができる。
【００１４】
【発明の実施の形態】本発明の好適な実施形態によれば、上記携帯機器／端末は、携帯電話回線網又はＰＨＳ回線網等の公衆回線に接続可能な携帯電話機、ＰＨＳ電話機又はＰＤＡ機器からなり、指紋認証センサを備えた指紋認証部と、役務又は機器の提供者側の受信装置と通信可能な近距離無線発信装置とを備える。好ましくは、指紋認証センサは、携帯機器／端末の外装部材に一体的に取付けられた静電容量式又は光学式の指紋認証センサからなり、携帯機器／端末は、ＩＣカード部を有する。ＩＣカード部は、特定人物（携帯機器／端末の所有者等）の指紋情報を格納した指紋情報格納部と、アクセス許可信号を送信すべき外部機器の情報を格納した外部機器情報格納部とを備える。指紋照合手段は、指紋認証部

又はＩＣカード部の少なくとも一方に組み込まれ、指紋認証センサの指紋検出結果と本人の指紋情報とを対比照合する。ＩＣカード部は、指紋の検出結果が本人の指紋情報と一致するとき、アクセス許可信号の発信を近距離無線発信装置に指令する。更に好ましくは、受信装置及び発信装置は、暗号化した信号を相互通信する。

【００１５】本発明の好適な実施形態において、上記受信装置は、建築物ドアの施錠装置、車両ドアの施錠装置、インターネットショッピングの端末、各種の自動販売機又は券売機、金庫又はロッカー等の施錠装置、公的書類交付用の本人確認装置、ＰＣ又は業務用ＣＰＵ等の如く、アクセス権を要する各種外部機器に配設される。これらの外部機器に設けられた受信装置は、携帯機器／端末の近距離無線発信装置が発信するアクセス許可信号を識別し、適宜セキュリティシステムを解除し、装置本体を利用可能な状態に移行する。

【００１６】本発明の他の好適な実施形態によれば、携帯機器／端末は、携帯電話機又はＰＨＳ電話機からなり、携帯電話機又はＰＨＳ電話機の所有者（契約者）は、電話機の指紋認証機能を利用して各種製品を購入し、或いは、所望のサービスの提供を受ける。製品購入又はサービス利用の対価は、課金情報として電話会社に通知される。電話会社は、課金情報に基づき、製品又はサービスの提供者に代わって電話料金と共に携帯電話機の所有者に料金請求し、所有者は、これを電話会社に対して支払う。

【００１７】本発明の更に他の実施形態として、ＡＴＭ等の金融機関端末から所望の金額を電子マネーとして携帯機器／端末にチャージしても良い。製品販売者又は役務提供者は、携帯機器／端末のアクセス許可信号により本人確認を行うとともに、携帯機器／端末にチャージされた金額を確認した上で、製品購入又はサービス利用等を許可する。他方、携帯機器／端末の所有者又は正規ユーザは、チャージした金額の範囲内において、購入製品又は提供役務の対価を電子マネーにより製品販売者又は役務提供者に支払うとともに、製品を購入し、或いは、サービスを利用する。

【００１８】

【実施例】以下、添付図面を参照して、本発明の好適な実施例について詳細に説明する。図１は、本発明の実施例に係る本人認証装置を構成する携帯電話機の概略正面図であり、図２は、図１に示す携帯電話機の内部構成を概略的に示すブロック図である。

【００１９】図１に示す携帯機器／端末は、携帯電話の公衆回線網に接続可能な汎用の携帯電話機１により基本的に構成され、携帯電話機としての一般的構成要素、即ち、ダイヤルキー２、各種ファンクションキー３、送話口４、受話口５、送受信アンテナ６及び液晶ディスプレイ７等を備える。携帯電話機１は更に、指紋認証部１０及び無線インターフェイスＬＳＩ１２を備える。

【００２０】本実施例では、指紋認証部１０を構成する静電容量式指紋認証センサ１１が、液晶ディスプレイ５の上方に配置される。指紋認証センサ１１は、指紋のパターンや特徴を電気信号に変換可能な多数のセンサ回路を備える。指紋認証センサ１１の被接触面（検出面）は、携帯電話機１のケーシング正面に露出しており、ユーザは、指紋認証時に所定の手指を指紋認証センサ１１の表面に当接する。指紋認証センサ１１は、被接触面、配線層及び基板とを板厚数mm程度の薄板形態に一体化した指紋検出／照合手段を構成し、指と接触した際に各センサ回路の静電容量を測定し、指紋のパターンや特徴を検出する。指紋認証センサ１１の基板には、認識処理デバイスが組み込まれ、認識処理デバイスは、指紋認識処理及び指紋照合処理を実行する論理回路を備える。

【００２１】無線インターフェイスＬＳＩ１２は、例えば、携帯電話機１のケーシング頂部に取付けられ、外部機器に配設された受信装置（図示せず）と数mの近距離で相互データ通信を行い、受信装置にアクセス許可信号を送信する。無線インターフェイスＬＳＩ１２として、１チップ型ＢｌｕｅｔｏｏｔｈインターフェイスＬＳＩ等の短距離無線通信デバイスを好適に使用し得る。受信装置も又、１チップ型ＢｌｕｅｔｏｏｔｈインターフェイスＬＳＩ等の短距離無線通信デバイスにより構成することができる。

【００２２】携帯電話機１の制御系は、図２に示す如く、上述の指紋認証部１０及び無線インターフェイスＬＳＩ１２を含むとともに、携帯電話機能部１５及びＩＣカード部１３を更に備える。

【００２３】携帯電話機能部１５は、携帯電話機１の一般的機能、即ち、キー入力による初期条件設定及び操作指示を携帯電話機１の各部に伝達するキー入力制御手段と、ダイヤル信号送受信及び音声送受信を制御する送受信制御手段とを備える。携帯電話機能部１５は更に、ＩＣカード部１３の判定結果に基づいて、不正使用の可能性を判定する使用禁止判定手段と、該判定手段が不正使用の可能性を判定したきに携帯電話機１自体の使用を強制的に禁止する使用禁止手段とを備える。

【００２４】携帯電話機能部１５に接続されたＩＣカード部１３は、判断プログラムを格納したＲＯＭと、判断プログラムの作業領域として機能するＲＡＭと、所定の正規ユーザ情報を格納したユーザ情報格納部と、外部機器情報を格納した外部機器情報格納部と、判断プログラムを実行し且つアクセス許可信号等を出力するマイクロプロセッサ及びインターフェースとを備える。判断プログラムは、外部機器に対するアクセス許可信号の出力可否を判定するように構成される。正規ユーザ情報は、予め登録された正規ユーザの指紋情報（指紋のパターン及び特徴等）を含み、外部機器情報は、アクセス許可信号を送信可能な外部機器に関する各種情報を含む。

【００２５】ＩＣカード部１３のインターフェイスは、

無線インターフェイスＬＳＩ１２に接続されるとともに、指紋認証部１０に接続される。指紋認証部１０は、上記指紋認証センサ１１の測定結果を指紋情報としてデータ処理する認識処理手段を備えるとともに、指紋認証センサ１１及び認識処理手段により得られた指紋情報（指紋パターン・特徴）に基づいて本人認証プログラムを実行する照合処理手段を備える。認識処理手段は、指の接触時に指紋認証センサ１１の各センサ回路の静電容量を測定し、これをデータ処理して指紋のパターン及び特徴を検出する。照合処理手段は、認識処理手段が検出した指紋情報と、ＩＣカード部１３に予め記憶された正規ユーザの指紋情報とを照合し、照合判定の結果を認証信号又は非認証信号としてＩＣカード部１３に出力する。

【００２６】図３は、指紋認証部１０が実行する本人認証プログラムの概要を示すフローチャートであり、図４は、ＩＣカード部１３が実行する判断プログラムの概要を示すフローチャートである。

【００２７】指紋認証部１０の指紋照合手段は、指紋認証センサ１１及び認識処理手段の指紋検出結果（指紋情報）と、ＩＣカード部１３の本人指紋情報とを読込み（S1）、両者を対比照合し(S2)、指紋の検出結果が正規ユーザの指紋情報と一致するとき、正規ユーザのアクセスを意味する本人認証信号をＩＣカード部１３に入力し(S3)、他方、指紋の検出結果が正規ユーザの指紋情報と一致しない場合、本人確認不能を意味する非認証信号をＩＣカード部１３に入力する(S4)。

【００２８】ＩＣカード部１３は、携帯電話機能部１５の初期設定及びキー入力設定を読み込むとともに、指紋認証部１０から入力された信号の種別を読み込む(S11)。ＩＣカード部１３は、本人認証信号の入力を検出したとき、初期設定又はキー入力設定によるマニュアル設定条件の成立を更に判定した上で、アクセス許可信号の出力を無線インターフェイスＬＳＩ１２に指令する(S13)。例えば、マニュアル条件設定により、外部機器へのアクセス禁止等がマニュアル設定されている場合、或いは、パスワード入力等の他の条件を付加的に要求するようなマニュアル設定がなされている場合、ＩＣカード部１３は、マニュアル設定条件の成立を判定し、このようなマニュアル設定条件が成立した場合にのみアクセス許可信号の送信を無線インターフェイスＬＳＩ１２に指令する(S14)。無線インターフェイスＬＳＩ１２は、ＩＣカード部１３からの信号に基づき、アクセス許可信号を外部機器に無線で発信する。

【００２９】他方、ＩＣカード部１３は、本人認証信号の入力を検出せず、非認証信号の入力を検出したとき(S15)、指紋不一致を示す判定結果を携帯電話機能部１５の使用禁止判定手段に出力する(S16)。使用禁止判定手段は、ＩＣカード部１３が指紋不一致の判定結果を比較的長時間に亘って継続的又は繰返し出力する場合、不正使用の可能性を判定し、携帯電話機１の使用を強制的に禁止するよう上記使用禁止手段に指令する。

【００３０】図５は、上記携帯電話機１の使用形態を例示する概念図である。携帯電話機１による指紋認証結果を用いてアクセス権を得るための外部機器として、例えば、建築物のドアの施錠装置２１、車両ドアの施錠装置２２、インターネットショッピングの端末２３、各種の自動販売機又は券売機２４、金庫又はロッカー等の施錠装置２５、公的書類の交付のための本人確認装置２６、携帯ＰＣ等の携帯端末２７、更には、業務処理用コンピュータ又はワークステーション２８等を例示し得る。これらの外部機器２１～２８には、携帯電話機１の無線インターフェイスＬＳＩ１２と通信可能な無線インターフェイスＬＳＩが付加的に取付けられ、或いは、機器本体に組み込まれる。

【００３１】ＩＣカード部１３の外部機器情報格納部は、各外部機器２１～２８の種別、セキュリティ機能及び認証機能等を具体的に記憶しており、無線インターフェイスＬＳＩ１２は、外部機器２１～２８と通信し、外部機器２１～２８が受信可能なアクセス許可信号を外部機器２１～２８に送信する。アクセス許可信号を受信した外部機器２１～２８は、携帯電話機１の本人認証機能により本人確認がなされたことをアクセス許可信号によって認知し、正規のアクセス許可信号を受信した場合、セキュリティシステムを解除し、利用可能な状態に移行する。即ち、建築物、車両ドア、金庫又はロッカー２１、２２、２５の施錠装置においては、施錠を解錠し、自動販売機２４又は公的機関の本人確認装置２６では、所望のサービスの提供を可能し、また、携帯端末２７又は業務用コンピュータ２８にあっては、データアクセス、ログイン又はデータ通信等の利用を可能にする。

【００３２】このような使用形態によれば、携帯電話機１の正規ユーザは、鍵又はカード、或いは、印鑑又は身分証明書等を常時携帯することなく、しかも、複雑なＩＤ番号及び暗証番号を記憶することなく、携帯電話機１のみを携帯することにより、本人であることを比較的容易に証明することができる。しかも、本人であることの証明は、極めて確実で偽造し難い手段、即ち、指紋の照合により行われるので、アクセス許可又はセキュリティシスムテム解除は、極めて安全に実施される。

【００３３】図６は、上記携帯電話機１の他の使用形態を例示する概念図である。図６に示す使用形態では、携帯電話機１の所有者は、携帯電話機１の指紋認証機能を利用して各種製品を購入したり、或いは、所望のサービスの提供を受ける。携帯電話機１の所有者（契約者）は、携帯電話機１のアクセス許可信号によりアクセス権の有無を識別可能な任意の製品購入手段又はサービス利用手段を利用し得る。製品購入又はサービス利用の対価、即ち、製品購入料金又はサービス利用料金は、課金情報として電話会社に通知され、電話会社は、これを集

計し、携帯電話機１の電話利用料金と一緒に定期的に携帯電話機１の所有者に料金請求し、所有者は、所轄の電話会社営業所、銀行又はコンビニエンスストア等で料金を支払う。他の支払い形態として、料金請求額を銀行自動引落しにより決済することも可能である。なお、上記課金情報は、携帯電話機１にも通知され、携帯電話機１のメモリは、これを記憶する。

【００３４】このような料金請求システムによれば、製品販売者又はサービス提供者の料金回収を電話会社が代行し、しかも、これを電話料金と共に一括して回収することができ、また、携帯電話機１の所有者は、個々の製品の購入時又はサービス利用時に現金を支払うことなく、各料金を後日に一括して決済することができる。

【００３５】以上の如く、本実施例に係る携帯電話機１は、従来の携帯電話機の基本構成に加えて、指紋認証部１０及びＩＣカード部１３、即ち、指紋認証装置（指紋検出手段、指紋照合手段及び指紋記憶手段）を組み込んだ構成のものであり、携帯電話機１の所持者は、信頼性及び確実性が高い指紋認証により本人認証を行い、これにより、各種の外部機器に対するアクセス権を得ることができる。本実施例の携帯電話機１によれば、従来の携帯電話機に潜在した課題、即ち、携帯電話機の使用者が必ずしも本人と一致しないという課題を克服し得るばかりでなく、最近の傾向として一人一台の割合で普及し且つ業務上又は私的な用途を多様な分野に急速に拡大しつつある携帯電話機を本人認証装置として使用することにより、多彩な分野に適応可能な利便性を備えた本人認証装置を提供することができる。

【００３６】また、本実施例の携帯電話機１は、外部機器と通信可能な無線インターフェイスＬＳＩ１２、即ち、無線発信装置を有し、アクセス許可信号は、携帯電話機１と外部機器とをケーブル接続することなく、外部機器に出力される。これは、音声又はデータを入出力する際に携帯電話機を外部機器にその都度ケーブル接続していた従来の携帯電話機と対比すると、適用範囲又は応用範囲を大幅に拡大するので、実用的に極めて有利である。

【００３７】かくして、上記構成の携帯電話機１は、携帯電話機一般の基本機能と、指紋認証装置による本人認証機能と、無線発信装置のアクセス許可信号発信機能との３つの機能を備えており、発信元が確実なアクセス許可信号を無線通信により多種多様の外部機器に送信し、多くの外部機器のアクセス権を一元的に確保する。従って、本実施例によれば、一般に普及している携帯電話機を利用した本人認証装置を提供し得るばかりでなく、多様な分野のアクセス権を一元化する本人認証方法を提供することができるので、携帯電話機１の所有者又は契約者は、大きな利便性を得ることができ、実用的に極めて有益である。

【００３８】以上、本発明の好適な実施例について詳細に説明したが、本発明は上記実施例に限定されるものではなく、特許請求の範囲に記載された本発明の範囲内で種々の変形又は変更が可能であり、該変形例又は変更例も又、本発明の範囲内に含まれるものであることは、いうまでもない。

【００３９】例えば、上記実施例においては、指紋を検出する検出面と認識処理デバイスとを一体化した構成の指紋認証センサについて説明したが、認識処理デバイスの機能を指紋認証センサから分離し、ＩＣカード部に組み込んでも良い。

【００４０】また、指紋を検出し且つ照合する上記認識処理手段及び照合処理手段の機能や、本人の指紋データを登録し且つ外部機器情報等を記憶する上記ユーザ情報格納部及び外部機器情報格納部の機能、更には、判断プログラムを実行し且つアクセス許可信号を出力するＩＣカード部の機能等の全てを単一のデバイス又はチップ（ＬＳＩ）に組み込み、単一のデバイス又はチップにより指紋認証プログラムを実行することも可能である。

【００４１】更に、上記携帯電話機による本人認証は、指紋照合のみにより行っても、或いは、指紋照合と、他の任意の本人確認手段、例えば、４桁程度のキー入力暗証番号の照合、或いは、携帯電話機の音声変換機能を利用した声紋照合等を併用しても良い。

【００４２】また、上記実施例では、認証機器として静電静電容量式の指紋認証センサを用いた構成を説明したが、光学式指紋認証センサを認証機器として採用しても良く、また、指紋認証センサを搭載する機器は、携帯電話機に限定されるものではなく、ＰＨＳ電話機やＰＤＡであっても良い。

【００４３】

【発明の効果】以上説明したとおり、本発明の上記構成によれば、各種機器及びサービスへのアクセス権を一元的且つ集約的に確立し得る本人認証装置及び本人認証方法を提供することが可能となる。

【図面の簡単な説明】

【図１】本発明の実施例に係る本人認証装置を構成する携帯電話機の概略正面図である。

【図２】図１に示す携帯電話機の内部構成を概略的に示すブロック図である。

【図３】図２に示す指紋認証部が実行する本人認証プログラムの概要を示すフローチャートである。

【図４】図２に示すＩＣカード部が実行する判断プログラムの概要を示すフローチャートである。

【図５】本人認証装置を構成する携帯電話機の使用形態を例示する概念図である。

【図６】本人認証装置を構成する携帯電話機の他の使用形態を例示する概念図である。

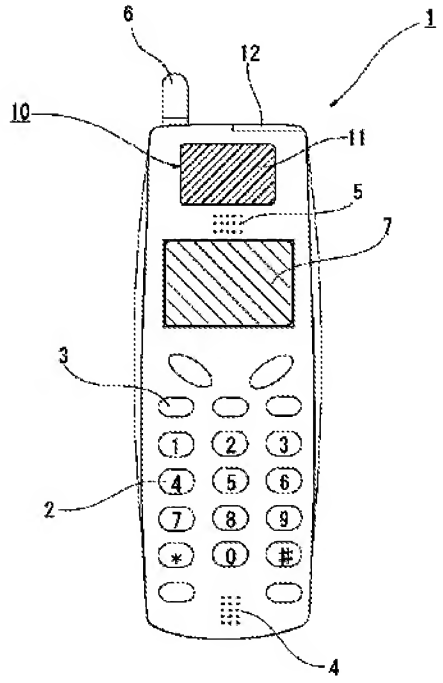
【符号の説明】

１　携帯電話機

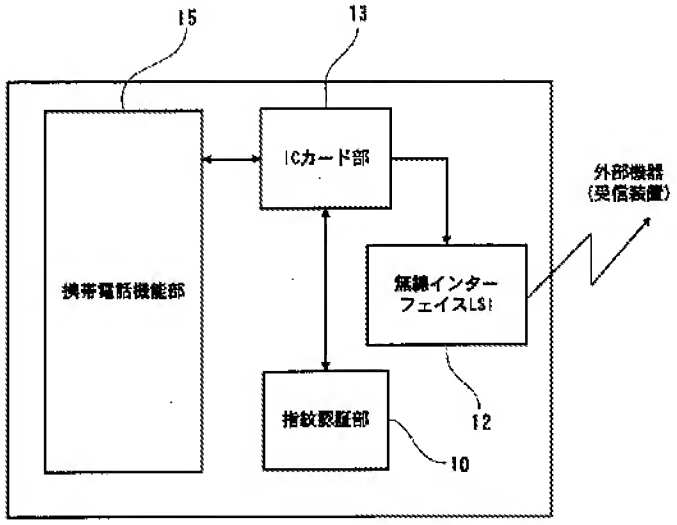
１０　指紋認証部

１１　指紋認証センサ
１２　無線インターフェイスＬＳＩ
１３　ＩＣカード部
１５　携帯電話機能部

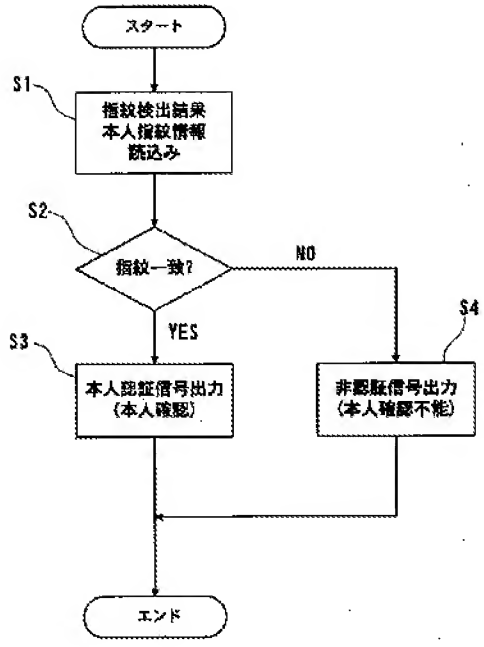
【図１】



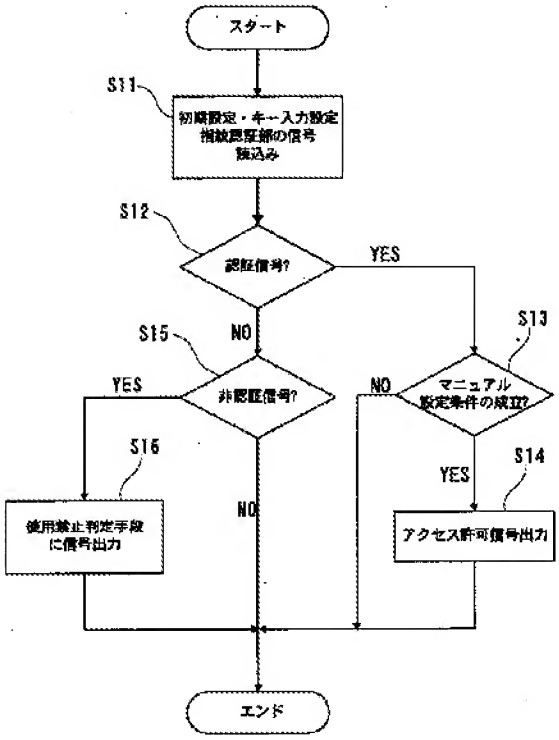
【図２】



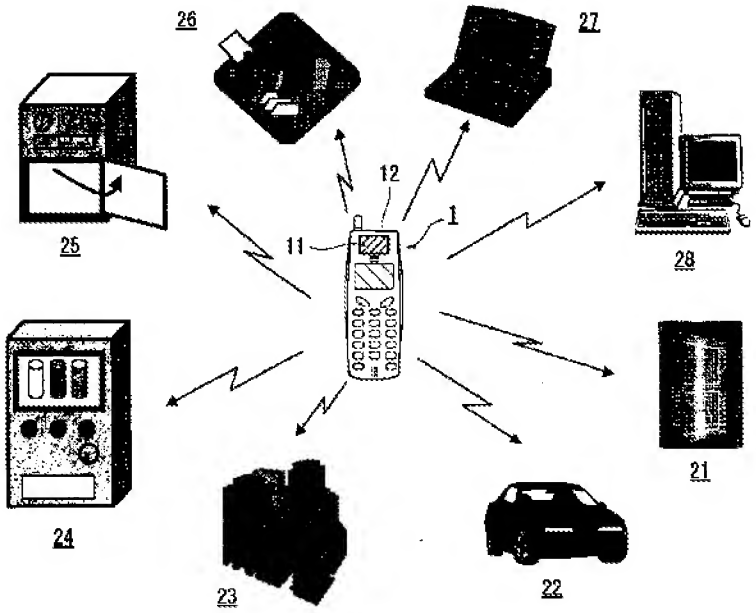
【図３】



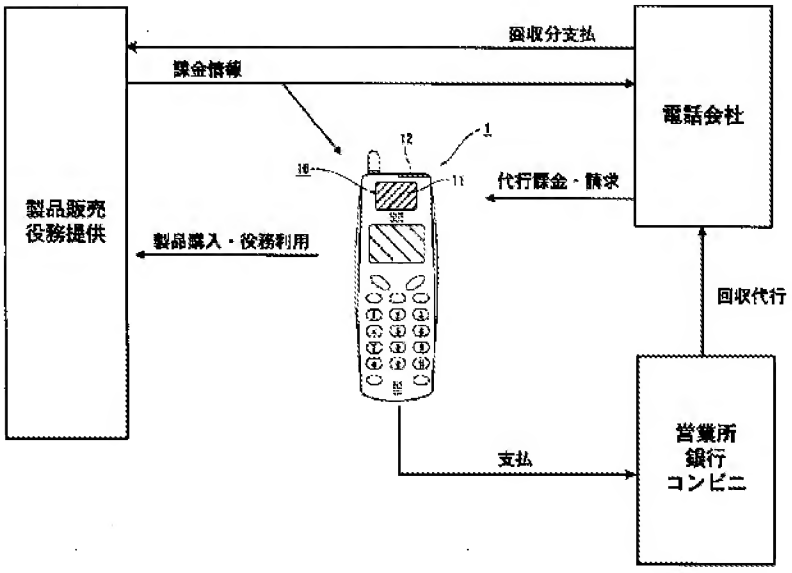
【図４】



【図5】



【図6】



フロントページの続き

(51)Int.Cl.⁷	識別記号	FI	テーマコード(参考)
H04M 1/725		H04B 7/26	109R 5K101
11/00	302	H04L 9/00	673D
			673E

(72)発明者　中山　俊一
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(72)発明者　塚田　悦司
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(72)発明者　瀧本　慶一郎
東京都千代田区大手町二丁目３番６号　株式会社三菱総合研究所内
(72)発明者　高橋　知樹
東京都千代田区大手町二丁目３番６号　株式会社三菱総合研究所内

Ｆターム(参考)　5B085 AE23 AE26
5J104 AA07 KA01 KA17 NA35 NA36 NA40 NA43 PA10 PA11 PA12 PA16
5K027 AA11 EE03 HH21 HH23
5K036 AA07 DD26 DD32 DD48 KK09
5K067 AA29 AA30 BB04 EE02 EE35 FF02 HH23 KK15
5K101 LL01 LL12 NN01 NN05 NN11 NN21

Last updated: 26.04.2011 Worldwide Database 5.7.22; 93p